



DEPARTMENT OF THE NAVY  
DIRECTOR NAVAL RESERVE INFORMATION SYSTEMS OFFICE  
2251 LAKESHORE DRIVE  
NEW ORLEANS, LOUISIANA 70145-0001

NAVRESINFOSYSOFFINST 5239.1B  
N123  
08 Sep 2000

NAVRESINFOSYSOFF INSTRUCTION 5239.1B

Subj: INFORMATION ASSURANCE SECURITY GUIDELINES

Ref: (a) SECNAVINST 5239.3  
(b) OPNAVINST 5239.1B  
(c) NAVSO P-5239-01  
(d) COMNAVRESFORINST 5239.1A  
(e) NAVSO P-5239-04  
(f) NAVSO P-5239-07  
(g) NAVSO P-5239-08  
(h) CNO Washington DC 212001Z Jul 95  
(i) DoD 5500.7-R  
(j) COMNAVRESFORINST 5239.2  
(k) COMNAVRESFOR New Orleans 161106Z May 00  
(l) SECDEF Washington DC 211930Z Oct 98  
(m) NAVSO P-5239-29  
(n) SECNAVINST 5211.5D  
(o) ASD (C3I) Memo of 16 Jan 97  
(p) CNO Washington DC 111754Z Oct 95  
(q) Advisory 97-10 DoD Site Licensed Anti-Virus Tools  
(r) NAVSO P-5239-19  
(s) COMNAVRESFOR P4000.1  
(t) Public Law 100-235, Computer Security Act of 1987  
(u) NAVRESINFOSYSOFFINST 5236.1A  
(v) NAVRESINFOSYSOFFINST 4400.1

Encl: (1) Computer Incident Report  
(2) Warning Banner Notice and Consent Log-on Banner

1. Introduction. The Department of the Navy (DON) Information Assurance (IA) Security Program is designed to comply with, Department of Defense (DoD), and DON IA policies per references (a) through (c). The Naval Reserve Information Systems Office (NAVRESINFOSYSOFF) IA Program is driven by a need to reduce system resources risk by identifying their vulnerabilities to specific threats and apply security measures to prevent or reduce the impact on system assets from threat occurrences. NAVRESINFOSYSOFF's IA Program is directed to ensure that information is protected from unauthorized disclosure, denial of service, destruction, and modification.

2. Purpose. The purpose of this instruction is to clearly communicate to all NAVRESINFOSYSOFF personnel that IA is multi-departmental, multi-disciplinary, and multi-organizational. NAVRESINFOSYSOFF personnel will be specifically charged with the responsibility of IA to achieve appropriate levels of security.

3. Scope. The information contained in this document applies to all NAVRESINFOSYSOFF Local Area Network (LAN) and Information System (IS) users including military, civilian, and contractor personnel. This instruction defines the laws, rules, significant directives, policies, and practices that will govern NAVRESINFOSYSOFF's IA Program, and will set guidance for NAVRESINFOSYSOFF's authorized users. For the purpose of this document, resources are to include all computer systems, microcomputers, notebooks, laptops, etc., and any workstations under NAVRESINFOSYSOFF cognizance.

4. Background. The security challenges confronting Navy information and ISS are multiplying rapidly with the exponential growth of interconnected systems

08 Sep 2000

for producing and exchanging data and information. As interconnectivity increases and the threats to information and ISs become more sophisticated and diverse, Navy systems become inherently more vulnerable to unauthorized access and malicious attacks and must be adequately protected.

5. Discussion. Policies are the primary building blocks for all IA efforts. To be successful, a set of policies must be implemented which establishes both direction and management support. The number one key to IA success is the involvement and support at all levels of management.

a. The Designated Approving Authority (DAA) decides if an IS network or computer resource may operate per references (a) through (c). Permission to operate is granted when the DAA determines that an IS operates at an acceptable level of risk.

b. The Director of NAVRESINFOSYSOFF is the DAA who is responsible for ensuring compliance with the DON IA Program.

c. NAVRESINFOSYSOFF's Information System Security Managers (ISSMs) and the Information Security (INFOSEC) staff consist of Information System Security Officers (ISSOs) and the Network Security Officer (NSO) which have been identified per references (d) through (g). The IA staff is further identified below:

(1) NAVRESINFOSYSOFF ISSMs function as the activity's focal point and principal advisors for IA matters on behalf of the DAA. The ISSMs report to the DAA and implement the overall IA Program as approved by the DAA.

(2) The ISSOs act on behalf of the ISSMs to ensure compliance with the IA procedures within their area of responsibility at their operation sites or facilities.

(3) The NSO acts on behalf of the ISSMs to implement the network security policy of the activity across all data networks and the activities connected to the data network.

6. Internet Policy. The current explosive growth of the Internet and the Information Superhighway creates a rapidly changing situation where boundaries between appropriate and inappropriate uses can be blurred. Some institutions have lost stature due to widely-circulated reports of clearly inappropriate activities being conducted on their computer systems and/or repeated break-ins resulting in compromise of their information resources. This situation requires that NAVRESINFOSYSOFF establish clear and explicit policy on appropriate and acceptable uses of its ISs per references (h) through (l).

a. NAVRESINFOSYSOFF authorizes use of its information resources for all purposes reasonably related to accomplishing its mission; intellectual inquiry intended to expand knowledge of current technology and keep abreast of technological innovations which may be of use to current or future customers; and to communicate electronically with customers, support contractors, vendors, and other agencies with whom the command has an association, so long as that communication is for official purposes. NAVRESINFOSYSOFF staff and contractors are encouraged to make maximum usage of these resources to increase their professional knowledge, skills, and ability to contribute to mission accomplishment; and identifying and implementing cost-effective, more efficient ways of performing assigned tasks.

b. NAVRESINFOSYSOFF restricts those uses of its information resources that are clearly inappropriate or which are inconsistent with the professional standards expected of its staff and contractors. In any instance, involving a question as to whether a specific action or conduct is or was appropriate, the

primary consideration should be whether such action or conduct would be consistent with that expected of professional military members and public servants. Personnel must realize that their actions reflect not only on themselves, but on NAVRESINFOSYSOFF, the Navy, and DoD.

c. Users have no expectation of privacy when using command information resources or public switched network (e.g., Internet, FTS-2000, etc.). Use of command resources and network connections constitutes express consent by the user to monitoring, recording, and auditing for the purposes of:

- (1) Ensuring the systems and networks are functioning properly.
- (2) Protecting against unauthorized access or use.
- (3) Ensuring the confidentiality, integrity of data and information resident on the systems and networks.
- (4) Ensuring that any software used complies with copyright agreements per references (m) and (n).

#### 7. Specific Restrictions and Limitations

a. There are certain activities not in keeping with NAVRESINFOSYSOFF mission or its status as a Navy activity that are expressly prohibited on all NAVRESINFOSYSOFF systems or those systems owned by customers or contractors that are operated on behalf of NAVRESINFOSYSOFF. These are:

- (1) Illegal, fraudulent, or malicious activities, partisan political activity, political or religious lobbying, and activities on behalf of organizations having no affiliation with NAVRESINFOSYSOFF. Actions which intentionally cause damage to equipment or introduction of viruses are included in this category.
- (2) Activities for the purposes of personal or commercial financial gain, and not in support of NAVRESINFOSYSOFF or its mission. Chain letters, solicitation of business or services, sales of personal property, resumes, and other forms of employment applications, etc., are not considered in support of NAVRESINFOSYSOFF or its mission.
- (3) Storing, processing, or displaying offensive, disrespectful, or obscene material, such as pornography and other sexually explicit material, hate literature, etc.
- (4) Storing or processing classified information on any system not explicitly approved for classified processing.
- (5) Annoying or harassing another individual, i.e., by sending uninvited E-mail of a personal nature or by using lewd or offensive language.
- (6) Using another individual's account or identity without their explicit permission, i.e., by forging E-mail, logging onto a system/network using their identification and password, cracking other users passwords, etc.
- (7) Viewing, damaging, or deleting other users files or communications without appropriate authorization or permission.
- (8) Attempting to circumvent or defeat security or auditing systems, without prior authorization from the command ISSMs or other than as part of legitimate system test or security search. This includes removing or tampering with virus checking capabilities as configured by Network Administrators; ISSMs, ISSOs, and NSO without prior approval or acceptance.

(9) Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's license agreement (i.e., activities that are commonly called "piracy").

(10) Installing legal copies of software expressly prohibited by the Director or by other competent higher authority, without prior permission. Any software purchased by an employee must comply with the software license and registration agreement and be documented with the command Software Manager (NAVRESINFOSYSOFF (N24)). This applies to public domain, customer-owned, personally-owned, government-owned, and shareware software. The Director's approval is assumed on all software procured by the command regardless of the funding source.

(11) Electronically transmitting classified or sensitive information to unauthorized recipients.

(12) NAVRESINFOSYSOFF networks shall not be used to transmit any communication where the meaning of the message, or its transmission or distribution, would violate any policy, applicable law, or regulation that would likely be highly offensive to the recipient or recipients thereof.

b. There are certain other activities which are not absolutely prohibited, but are almost always inappropriate. Individuals engaging in such conduct may reasonably expect to be asked to justify their activities, and if reasonable justification does not exist, may find their judgement and/or professional standards seriously questioned. Examples of such generally inappropriate activities are:

(1) Use of NAVRESINFOSYSOFF systems that, in the judgment of the responsible system administrator, seriously interfere with other legitimate uses or users. Examples may include "hogging" systems or actions which cause excessive network slowdowns, excessive large file transfers, excessive personal E-mail, and excessive storage of large (i.e., multi-media) non-mission related files.

(2) Storing files or material which could reasonably be used for illegal or fraudulent purposes.

c. Users who participate from NAVRESINFOSYSOFF systems in news groups, bulletin boards, discussion lists, etc. should generally limit such participation to forums related to their own professional expertise or assigned projects and should ensure their contributions are restrained, professional, objective, and clearly identified as personal opinions, not official NAVRESINFOSYSOFF, DON, or DoD policies.

8. Firewall. Per reference (h) all Navy ISs with servers, including web servers, which are connected to unclassified publicly accessible computer networks, such as the Internet, will employ appropriate security safeguards (e.g., a Firewall) as necessary to ensure the integrity, authenticity, privacy, and availability of a command's IS and its data. A Firewall that is properly installed, configured, and maintained can be expected to perform reliably per the policies, rules, access lists, and authorization criteria that have been established and set up for its effective operation.

9. WebPage Access. WebPages provide the public with user-friendly graphics based multi-media access to information on the Internet, and is the most popular means for accessing, storing, and linking Internet-based information in practically any format. Information placed on any NAVRESINFOSYSOFF WebPage shall be unclassified, have a clearly defined purpose related to the mission of the organization per reference (l), and strive to be accurate and current.

10. E-mail Policy. E-mail provides an effective way to pass and chronicle organizational communications. The following policy clearly describes

NAVRESINFOSYSOFF command guidelines regarding access to and the disclosure of messages sent or received by employees while using the command's E-mail system per references (h) through (k). The intent of this policy is to reinforce the notion that each user should have their own E-mail account, and that users should not share their accounts per references (h) through (k).

a. Passwords will be activated on all E-mail systems for individual users.

b. Management's Right to Access Information. The E-mail system has been installed by NAVRESINFOSYSOFF to facilitate command communications. Although each employee has an individual password to access this system, the contents of any E-mail is accessible at all times by NAVRESINFOSYSOFF for any official command purpose. The command does reserve the right to inspect, copy, store, and disclose the contents of E-mail messages at any time. However, it will do so only when it is believed to be appropriate to prevent or correct improper use, satisfy a legal obligation, or ensure proper operation of the E-mail facilities per references (h) through (k).

(1) The E-mail system may be subject to periodic unannounced inspections, and should be treated like other shared filing systems. All system passwords and encryption keys must be available to command ISSMs. Installation of encryption programs or encrypted files will not be used without first providing such appropriate keys to the ISSMs. Copies of all keys and passwords will be kept under restricted access, and be used for emergency or legitimate purposes at the direction of the department director, or by higher authority. All E-mail messages are command records, contents properly obtained for legitimate business purposes may be disclosed within the command without your permission. Therefore, you should not assume that messages are private. Back-up copies of E-mail are regularly completed, maintained, and referenced for official and legal reasons.

(2) When necessary for the maintenance of a system or network, system administrators may restrict availability of shared resources. It may also be necessary to access a user's files to resolve or follow-up on reported problems.

(3) Groupwise Attachments. The Information Technology Center has a 4MB size limit on attachments sent through GroupWise. Large files sent through GroupWise will slow the system down, delaying the receiving, and sending of E-mail. Large photograph files, graphics, and beer commercials have been recent culprits causing delays. Remember, this is a government E-mail system, and items being sent through GroupWise that are not authorized by the government could result in administrative and/or disciplinary action. This includes chain letters, beer commercials, and material considered offensive.

c. Personal use of E-mail. Some reasonable personal use of the IS may be authorized. Examples of authorized personal use include reasonable communications by civilian, military, and contract personnel while traveling on U.S. government business to notify family members of official transportation, or schedule changes. They also include personal communications from the employee's workplace that are reasonably made while at work, such as checking in with spouse, or minor children, scheduling doctor, automobile, or home repair appointments, brief Internet searches, etc.

(1) NAVRESINFOSYSOFF provides the E-mail system to assist in the performance of the command's mission. Incidental, and occasional personal use of E-mail may be permitted, but these uses shall not interfere with the mission of the command and will be treated the same as other messages. NAVRESINFOSYSOFF reserves the right to access and disclose as necessary all messages sent over its E-mail system, without regard to content. Since, personal messages can be accessed by NAVRESINFOSYSOFF management without prior

notice, E-mail should not be used to transmit any messages that you would not want read by a third party. For example, you should not use the command E-mail system for personal or medical information about yourself or others likely to embarrass the sender, or cause undue emotional duress of others. In any event, you shall not use these systems for such purposes of soliciting for commercial ventures, religious, political or personal causes, external organizations, or other similar, non-job-related solicitations. Misuse of any NAVRESINFOSYSOFF system may be subject to disciplinary action.

(2) Any user of the E-mail system whose actions involving E-mail that violate this policy, or any other related command policy or regulation, may be subject to limitations of E-mail privileges as well as other disciplinary actions.

d. Forbidden Content of E-mail Communications. Per reference (j), you may not use NAVRESINFOSYSOFF ISS in any manner that may be reasonably seen as insulting, disruptive, offensive by other persons, harmful to morale, or in any way detrimental to good order and discipline. Examples of forbidden transmissions include sexually-explicit messages, photographs, cartoons, or jokes, ethnic or racial slurs, messages that can be construed to be harassment, or any of the above which ridicules others based on their sex, race, sexual orientation, age, national origin, religion, or political beliefs. In addition, the following specific actions and use of E-mail are improper, and violations may result in disciplinary action (this list is not an all inclusive list):

(1) Sending government documents or work related messages to a private Internet Provider E-mail account (i.e., America Online (AOL), Bellsouth, etc.)

(2) Concealing or misrepresenting names or affiliations in E-mail messages.

(3) Altering source or destination address of E-mail.

(4) Using E-mail facilities for commercial or private business purposes, or "underground" organizations.

(5) Using E-mail which unreasonably interferes with or threatens other individuals.

(6) Using E-mail that degrades or demeans other individuals.

(7) Transmitting fraudulent, harassing, or obscene messages and/or materials. These messages are not to be sent, printed, requested, or stored.

(8) Congesting the E-mail system (e.g., numerous/large files).

(9) Transmitting chain letters and other forms of unapproved mass mailings.

(10) Storing or processing classified information on systems not explicitly approved for classified processing. Classified data is not permitted on the NAVRESINFOSYSOFF E-mail system.

(11) Downloading video and/or audio streaming from Web radio stations and other similar sites.

(12) Subscribing to mailing lists and Instant Messenger.

(13) Participating in Worldwide Chat rooms.

(14) Posting personal home pages.

11. Virus Scanning Policy

a. NAVRESINFOSYSOFF enforces anti-virus and virus eradication efforts to reduce the risk of introducing malicious codes into command owned/operated ISs, reduce any resultant damage, and contain the spread of such software per references (p) through (r). "A computer virus is malicious software which can hide itself in other executable software (including macros) and then cause that software to make copies of the virus."

b. To protect our IA assets against virus infection, we will use the three step approach:

(1) Prevention. Those steps necessary to limit or prevent exposure to viruses.

(2) Detection. Those steps necessary to detect infections to limit the spread and impact.

(3) Response/recovery. Those steps necessary to remove the virus and restore the ISs and files to normal operation.

c. The use of command anti-virus software is mandatory for any microcomputers. This includes all IS resources accessing from remote sites. Reference (q) identifies the current DoD site licensed approved anti-virus software for use on NAVRESINFOSYSOFF microcomputers and may also be used by all DoD personnel on their home personal computers. The anti-virus software shall be configured to scan the hard-drive(s) on first boot each day the system is turned on and remain memory Terminate-and-Stay-Resident (TSR), while the computer is in operation. Waivers for this requirement must be approved in writing by the ISSMs based on demonstrated and valid reason (insufficient memory, memory conflicts, or other conflicts with application software used on the system, etc.). System response time is not a valid justification for removing anti-virus scanning capabilities. The option will be to scan all files on the hard drive, not just program files.

d. Files downloaded from remote sources (BBS, networks, online service, etc.), or received on diskettes from sources outside this command shall be scanned for viruses upon receipt/download before being executed on any computer. Diskettes brought from users home computers are included in this category.

e. Any server that is connected to NAVRESINFOSYSOFF LAN must be protected by command standard anti-virus software.

12. Methods of Transmission. The most common method of spreading a virus from one computer to another is through the exchange of infected floppy diskettes. A virus can also be transferred by direct access to another computer (through a network or modem). The following are common sources of viruses:

a. Files downloaded from Bulletin Board Systems (BBSs), online services, and Internet sites.

b. Preloaded software shipped on a new computer.

c. Demonstration/evaluation software received from vendors.

d. Diskettes used by service or support technicians.

e. Pirated (i.e., illegal) software acquired from friends or co-workers.

f. Shareware diskettes received from mail order catalog companies.

08 Sep 2000

- g. Computer stores selling returned software as new.
- h. Diskettes used in friends or co-workers computers.
- i. Exchange of infected files on a network.
- j. Specific acts of sabotage by disgruntled employees.
- k. College campus computer laboratories.
- l. Using infected backups.
- m. Remote access to infected computers.
- n. Government-owned and distributed software.

13. Virus Protection

a. All ISSs (i.e., workstations, stand-alone, etc.) will load and use the latest version of virus scanning software authorized as provided by NAVRESINFOSYSOFF INFOSEC office.

b. All new incoming computers will be scanned and installed with the current authorized version of virus scanning software as part of the initial setup.

c. Users will acquaint themselves with the proper use of the virus scanning software to prevent the spread of computer viruses.

d. Departmental ISSOs will:

(1) Identify all microcomputers within their department and ensure the current approved anti-virus software is installed and operating.

(2) Compile all information needed to supply the Fleet Information Warfare Center's, Naval Computer Incident Response Team (NAVCIRT) with an Incident Report, as contained in enclosure (1) of this instruction.

e. ISSMs will:

(1) Ensure applicable information is provided to NAVCIRT in a timely, accurate manner.

(2) Conduct random software license, virus, and system audits.

(3) Provide the departmental ISSOs with updated versions of authorized virus scanning software.

(4) Ensure command IA training is provided.

14. Diskette Label. (External Labeling) Implementation requirements for the IA Program centers around the classes of data processed at NAVRESINFOSYSOFF and the requirements governing its protection. Central Processing Units (CPUs) will accurately reflect (label) the highest level of information stored and/or processed. NAVRESINFOSYSOFF personnel will label all diskettes with user name, extension, and department code.

15. Desktop Policy. To provide NAVRESINFOSYSOFF with the information necessary to operate and use their ISSs securely per reference (a), all NAVRESINFOSYSOFF personnel shall comply with and ensure ISSs within their area of responsibility are covered and comply with the procedures within this instruction.



- 08 Sep 2000

16. Information Assurance Custodian

a. To comply with references (a) and (s), NAVRESINFOSYSOFF uses the Control Equipage Inventory System (CEIS) to ensure proper accountability of controlled minor property (including hardware and software control, physical inventory distribution, and usage controls). Changes in the status of any NAVRESINFOSYSOFF property shall be completed per applicable laws, regulations, NAVRESINFOSYSOFF resource management policy, and documented by an individual Internal Transfer Worksheet (NAVRESINFOSYSOFF 5236/2), or other appropriate, authorized transfer documentation authorized by references (u) and (v). Per reference (u) only approved software will be installed on workstations. Only Telecommunications/Operations (NAVRESINFOSYSOFF (N5)) technicians will install commercial copyrighted software on microcomputers.

b. NAVRESINFOSYSOFF ISSs are authorized to process Official Use Only, Unclassified, and Sensitive Unclassified data. This security policy represents the minimum requirements for ISSs that process exclusively unclassified and sensitive unclassified data. Any changes in the level of data processed using NAVRESINFOSYSOFF equipment are not authorized without prior specific written approval from NAVRESINFOSYSOFF (N00) and ISSMs.

c. Desktop Support Team. Upon replacement or transfer of a desktop support team member all administrative passwords in use by that member will be changed.

17. Physical Security/Access Control. Most NAVRESINFOSYSOFF ISSs are located in government secured workspaces. All personnel are required to carry government issued coded identification badges. Each office door will be equipped with either a cipher lock, combination cipher lock, door key, or card access system. Personnel are responsible to ensure reasonable actions are taken to provide for physical security and access controls for all ISSs under their area of responsibility.

18. Good Security Practices. Password recommendations:

a. Change passwords frequently. The longer you use the same passwords, the higher the risk of compromise. Password changes of every 90 days is a good rule of thumb.

b. Use a combination of numbers and letters (capital and lower case too, if permitted). Do not use common words (i.e., password), persons (i.e., your name), places (i.e., NAVRESINFOSYSOFF), dates, numbers, or other words that can be closely identified with you.

c. At a minimum, use six to eight characters in length for passwords.

d. Safeguard and do not share passwords.

e. Have your E-mail (such as GroupWise) password protected.

f. Inspect your data and equipment. If you have reason to suspect someone may have tampered with your equipment, files, or data, report it immediately to your departmental ISSO or ISSM.

g. Do not leave sensitive data in an IS or on diskettes that does not afford adequate access controls or proper security.

h. Ensure all ISSs have adequate security measures, especially in unoccupied spaces.

i. Avoid keeping magnets, liquids, and food in the immediate vicinity of all ISSs. Foods and liquids dropped on or into ISSs (including keyboards) can

08 Sep 2000

cause malfunctions and destruction of property and files. Magnets are also capable of causing malfunctions and destruction of electronic files.

j. Report any suspected IS misuse or abuse to your departmental ISSO or ISSM. Whether directed against you or not, abuse or misuse of command IS resources hinders the timely completion of your task.

k. Ensure a password is active on your screen saver and the screen saver is activated after 5 to 10 minutes of system inactivity.

l. Logoff the network daily.

19. Standard Operating Procedures. All authorized individuals using IS equipment must be made aware of security procedures prior to operating any NAVRESINFOSYSOFF resource. The following procedures are applicable to all authorized users:

a. All diskettes, Compact Disks (CD), and software are to be secured during non-working hours and when not in use.

b. A warning label indicating the highest level of information processed in each IS will be affixed to the CPU.

c. Backup of all important data should be performed on a weekly basis or more often, if appropriate.

d. Ensure that each microcomputer is equipped with a surge protector.

20. Media Protection

a. Media (all diskettes, CD's and cartridge tapes) will be handled with care and stored in their protective jacket (if appropriate) at all times when not in use.

b. Protect from bending or similar handling. Do not use magnets, rubber bands, or paper clips which may cause damage.

c. Avoid contact with objects which have magnetic fields (i.e., telephone instruments).

d. Avoid writing with ball-point pens, pencils, or similar instruments either directly or through the protective jacket.

e. Label appropriately.

f. Do not force or bend media when inserting into a drive.

21. Media Input/Output Declassification and/or Destruction

a. All personnel are to ensure that hard copies of all Privacy Act (PA) data are properly stored and disposed of. Per reference (n), all users are to be aware of releasable information for NAVRESINFOSYSOFF personnel.

b. All diskettes that contain sensitive unclassified or personal information are to be adequately protected and should only be discarded in regular waste containers after ensuring the media and data has been adequately cleared or rendered useless.

22. Individual IS Contingency Planning (CP). CP is an integral phase of an activity's IA Program. CP is required for all ISs, networks, or other computer resources that are essential to the performance of an activity's mission. The following elements will assist all NAVRESINFOSYSOFF personnel

08 Sep 2000

tasked with providing information systems services during times of disruption of normal operations.

a. In the event your IS becomes inoperative:

- (1) Call the Customer Support Center (CSC) at 697-7070 or 1-800-537-4617.
- (2) Provide your name, building/room number, and extension.
- (3) Give a brief description of the problem.
- (4) Obtain the name of the CSC representative assisting you.
- (5) The CSC representative will provide you with a trouble service ticket number; refer to this number when any future inquiries are placed.

b. Any significant changes in hardware/software configuration, classification level of processed data, or operating mode/posture, requires a reevaluation of the IS, and should be promptly reported to your departmental ISSO or command ISSMs.

23. Warning Banner. DoD mandates the use of a warning banner on all ISs as stated in reference (o). The warning banner is intended to confirm to the user that all data contained on DoD systems are subject to review by DoD security and/or System Administrator personnel and ensure that computer users are aware of system monitoring. The lack of proper warning banners may result in the violation of federal wiretap and privacy statutes. This applies to all networked and stand-alone DoD systems, both government and contractor owned, that access government data files. The file and any updates are available from your departmental ISSO or ISSM. The banner should be displayed at system initialization. All personnel shall ensure that the banner is displayed on all systems (workstations, servers, stand-alone, etc.). Enclosure (2) of this instruction is provided for your information.

24. IA Training and Awareness. Reference (t) mandates training for all personnel responsible for the input and use of government resources. There shall be in place, a security training and awareness program for the security requirements for all persons accessing ISs per references (a) and (b). The INFOSEC staff will develop and maintain the NAVRESINFOSYSOFF IA program. The security training program will include a mixture of security videos, oral classroom presentations, annual awareness training (briefs), E-mail security messages, Plan of the Week (POW) notes, and security posters.

25. Responsibilities

a. All NAVRESINFOSYSOFF system users are responsible for adhering to the requirements of this instruction. Individual users who violate these requirements may be subject to various penalties, ranging from informal counseling, to revocation of NAVRESINFOSYSOFF IS user privileges and resources, to formal disciplinary action, including reprimands, fines, non-judicial punishment, court-martial of military personnel, or removal for cause of civilian/contractor personnel. In all cases, users are accountable for their actions.

b. Supervisors will ensure their employees are apprised of and read this instruction and be responsible for the use of the IS assets under their respective jurisdiction.

c. ISSMs will include training on the requirements of this instruction during indoctrination orientation and ensure refresher training during annual IA security training.

08 Sep 2000

d. Contracting Officer's Representatives (CORs) will apprise their contractors of this instruction and their responsibilities.

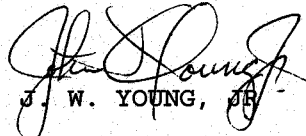
e. The LAN Administrator and NSO will monitor user's files and E-mail in cases where network/data security is in question and assist ISSMs with investigations as necessary.

f. The Software and Resource Manager will ensure that all software is accounted for, properly licensed, and any unauthorized software is promptly removed or legally licensed on all command ISS.

g. Privileged users are those having "super-user root" or equivalent access to a system which provides complete or near complete control of the operating system. To ensure the security and integrity of data, administrators have greater responsibilities to monitor, avoid, and prevent improper access to, and misuse of computational resources under their control.

26. Action. Supervisors will ensure that their employees are in receipt of and comply with this instruction. COR will ensure contractors are in receipt of and comply with this instruction. Actual or alleged violations of, or questions regarding to the applicability of this instruction will be addressed through normal command channels. The ISSMs will investigate any incidents that are security related. The Software Manager, with advice from the ISSMs, will make determinations concerning legal software usage issues. The DAA will make the final determination in all instances that cannot be adequately resolved at lower levels.

27. Forms. The NAVRESINFOSYSOFF 5236/2 (01-00), Internal Transfer Worksheet mentioned within this instruction is available from NAVRESINFOSYSOFF (N24) per references (u) and (v).

  
J. W. YOUNG, JR.

Distribution: (NAVRESINFOSYSOFFINST 5216.1)

Lists A, B and C.

CORs will provide contractors a copy for compliance

COMPUTER INCIDENT REPORT

1. The following information is provided on the Information System (IS) viruses.

(a) Name of infecting virus: Loveletters.ubs

(b) Source of the virus and date detected: The Loveletters virus was detected on one 3.5 inch diskette in the Administrative Department on 2 Jun 97. In an attempt to read a file, a diskette provided by NAVRESINFOSYSOFF (N55), the IBM Anti-Virus (IBMAV) software detected the Loveletters virus. When the user received the message "infected boot records were found", employee immediately notified the IS Security Officer who assisted in the documentation and virus removal.

(c) Other locations, within or outside of the command, was possibly infected as a result of this virus: None. The originator of the diskette was notified.

(d) Number and types of systems infected: One 3.5 inch diskette

(e) Method of clean-up: NORTON.NAV

(f) Number of man-hours required in effort: 5 minutes

(g) Damage or observations resulting from the virus triggering: None

(h) Command name and location:  
Director, Naval Reserve Information System Office  
2251 Lakeshore Drive  
New Orleans, LA 70145-0001

(i) Point of contact: (Reporting Information System Security Manager's Name)  
DSN: 647-1506 Commercial: (504) 697-1506

WARNING BANNER

NOTICE AND CONSENT LOG-ON BANNER

This is a department of defense DoD computer system. This computer system, including all related equipment, networks, and network devices (specifically including internet access), are provided only for authorized U.S. government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of their system. During monitoring, information may be examined, recorded, copied, and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of the system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes.